National Security Agency/Central Support Service

INFORMATION ASSURANCE DIRECTORATE

CGS Incident Response Capability

Version 1.1.1

Incident Response is a conscious plan of action given the stimulus of an assessed occurrence having actual or potentially adverse effects on an asset. It involves notification, triage, escalation, isolation, and restoration (when appropriate) of technical, personnel, physical, and environmental incidents. Incident Response provides the Capability to respond to any incident (both external to the network and information technology [IT] related). A formal Incident Response Team (IRT) provides the expertise to appropriately respond to the problem.

07/30/2012

CGS Incident Response Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Incident Response is a conscious plan of action given the stimulus of an assessed occurrence having actual or potentially adverse effects on an asset. It involves notification, triage, escalation, isolation, and restoration (when appropriate) of technical, personnel, physical, and environmental incidents. Incident Response provides the Capability to respond to any incident (both external to the network and information technology [IT] related). A formal Incident Response Team (IRT) provides the expertise to appropriately respond to the problem.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Incident Response Capability provides the Enterprise with the ability to respond to threats and attacks directed against it. Incident Response, in conjunction with other Capabilities, provides the full spectrum approach of monitoring, detection, analysis, and response. The Incident Response Capability specifically focuses on the ability to respond. Incident Response is both a strategic and tactical Capability that uses real-time information, provided from other Community Gold Standard (CGS) Capabilities, regarding the Organization’s domain and assets.

The Enterprise shall have a program, staff, and plan to address Incident Response. The Enterprise may obtain Incident Response services from other organizations, after executing the appropriate organizational agreements, or they may use their own technical staff to perform Incident Response actions. All staff conducting Incident Response shall be staff members dedicated to this practice and not performing these duties as collateral responsibilities.

The following definitions are important when discussing Incident Response. An event is an occurrence, not yet assessed, that may affect the performance of an information system. [CNSSI-4009] An incident is an assessed occurrence having actual or potential adverse effects on an information system. [CNSSI-4009] Incidents are a subset of events. An attack is an attempt to gain unauthorized access to an information system's services, resources, or information, or the attempt to compromise an information system's integrity, availability, or confidentiality. [CNSSI-4009] Attacks are a subset of incidents.

Incident Response employs a 24/7/365 operational ability to respond to the full spectrum of technical, personnel, physical, and environmental incidents or attacks. Each of the following incidents or attacks feeds into the overall Incident Response Capability:

- Technical–Related to the IT devices within the Enterprise (e.g., workstations, servers, routers, firewalls)
- Personnel–Related to the characteristics of people and their actions (e.g., illegal activities, clearance revocation, adverse personnel action, terrorist group affiliation)
- Physical–Related to facilities where the Enterprise has points of presence (e.g., building alarms, bomb threat, loss of electric power)
- Environmental–Related to occurrences in nature (e.g., hurricane, flood, earthquake)

A comprehensive Incident Response strategy consists of the ability to execute the following types of responses:

- Fully automated–The response is machine to machine from incident detection to action taken (e.g., firewall penetration results in disabling its network connection).
- Partially-automated–The response is determined by human involvement, then automatically executed (e.g., trouble call to help desk results in an automatic router table update); or the response is determined automatically, but must be manually implemented (e.g., equipment failure automatically detected, but requires manual repair or replacement).
- Manual–The response is determined and implemented with human involvement (e.g., supervisor report of unexplained employee absence results in a phone call to security to investigate).

Fully automated response shall be used whenever possible because it is the most timely and efficient. Technical incidents compose the bulk of incidents handled in this manner. Any of the four incident types that cannot be handled automatically are candidates for either semi-automated response or manual response, as required.

Characteristics of Incident Response include:

- Incident Response procedures, roles, and responsibilities of users and Incident Response personnel shall be documented. The scope of the Incident Response service shall be clearly defined.
- Planning and analysis shall take place prior to conducting Incident Response activities to ensure that properly skilled staff and the right resources are available when needed.
- Incident Response shall clearly identify and enumerate supporting services for the Incident Response process (e.g., a specialized team for treating viruses).
- Incident Response shall clearly identify and enumerate consumers of Incident Response outputs, including real-time data feeds during Incident Response.
- To support forensic investigation and Incident Response activities, a strict chain of custody shall be maintained for any physical evidence that must be confiscated or modified. The IRT has appropriate authority (in agreement with customer Organization) to conduct activities for forensic investigations, and all legal and procedural provisions are in place to do so.
- Real-time information shall include more than just details on the technical infrastructure, such as what missions are affected (see the Understand Mission Flows Capability).
- Incident Response shall be designed and implemented to facilitate interoperability with constituents. Reporting shall be in a standard format for consumption by peer or authority Organizations.
- Records of incidents shall be maintained in a centrally managed repository for the Enterprise.

Incident Response begins with notification of an event, incident, or attack to be addressed. Many, if not most technical incidents, are received and responded to automatically, in near real-time (i.e., as they occur). Incident notifications of all types also come from other Capability sources (see Capability Interrelationships).

The triage process assesses characteristics of the event, incident, or attack to determine its actual or potential adverse effect (either incident or attack) and whether it has occurred before (known) or not (new). The response to known incidents or attacks is the same as applied to previous incidents or attacks, which expedites resolution. New incidents or attacks are quickly identified for further investigation.

For incidents or attacks that cannot be resolved by standardized response procedure (e.g., help desk), formal procedures describe the escalation of incident or attack details to specialists for review, leading to determination of a course of action.

The next step is characterizing the affected portion of the system and possibly isolating it from further interaction. Based on mission impact, anomaly type and severity, and response team mission, there may be times when no immediate action is taken so that more knowledge can be obtained about the incident or attack as it continues to affect the system.

Incident Response concludes with restoration of mission functionality based on input from the Contingency Planning and Risk Mitigation Capabilities. Timeframes and methods for response depend on the incident or attack and input from the Risk Analysis Capability and mission requirements. The transition to Incident Analysis is a smooth one because the analysts are the same people involved in the triage process.

Throughout the Incident Response process, details on events, incidents, and attacks, and the response actions taken, are securely stored and maintained in a central data repository. The frequency of offloading or writing the information to the central repository is dependent on the organizational policy. At a minimum, the information on old incident shall be offloaded to ensure records of new incidents do not overwrite older information, and to ensure there is enough room to store new records on the local systems. The information is shared with other Capabilities and is discoverable and accessible in accordance with established information sharing policy for the Organization and requestor privilege and authority based on functional need.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Events are occurrences that must be examined immediately to determine if they are a problem.
2. Incidents are expected to happen despite appropriate preventative actions.
3. IRTs have sufficient system access and authority to respond effectively.
4. Awareness of how to use the Incident Response service is made available to the users within the Enterprise.

5. Incident Response procedures are formalized and personnel trained on how to engage Incident Response and initiate the Incident Response process.
6. Incident Response Capabilities at the agency and Organization levels have a line of communication with their internal and external Authority Organization(s), as defined by organizational policy.
7. Event Monitoring and Detection Capabilities must be implemented within the Enterprise.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability provides records of incidents to a central data repository for the Enterprise.
2. The Capability manages the flow of information about the incident based on the balance of need to share and need to know.
3. The Capability may not need to immediately execute a response for all incidents.
4. Not all incidents are attacks.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

For an Organization to successfully implement an Incident Response Capability or use an external Incident Response Capability, the elements of Incident Response (technical, personnel, physical, and environmental) will be appropriately synchronized and balanced. The Incident Response Capability cannot be realized with any one element dominating to the detriment of the others.

To assist the Organization in understanding and implementing, where appropriate, the Incident Response Capability, the following sections provide an elaboration of Incident Response implementation organized as Incident Response inputs, Incident Response process, and Incident Response outputs. Incident Response inputs are the event, incident, or attack notifications and are data feeds to the Computer Incident Response

Team (CIRT) or IRT. Outputs will take the form of real-time intelligence data, static reports, and recommendations, among others.

Incident Response Inputs–Incident Response inputs will be received and responded to automatically, in near real-time (as it occurs) and include:

- Escalation from help desk or other first line of filtration between an event detection and an Incident Response
- Automated ticketing system, which may include feeds from any number of Computer Network Defense (CND) related monitoring devices
- Data feeds from monitoring and detection mechanisms.

Incident Response Trigger Events–The number and type of trigger events depend on the vulnerabilities and threats to the system and are determined by the risk analysis based on these vulnerabilities and threats; the enumeration of trigger events, an output of the risk analysis; and the ability of front-end systems and processes to detect and provide notification of trigger events. Events that trigger the Incident Response process include, but are not limited to, the following:

- Automated detection of an anomaly (e.g., host-based intrusion detection system [HIDS] detects an anomaly that could be the presence of an intruder and sends a notification for subsequent investigation)
- Manual detection of an anomaly (e.g., upon initial logon attempt after returning from vacation, a user experiences a locked account message because of too many incorrect logins; the user notifies the help desk that someone was trying to use his or her account while he or she was on vacation)

Incident Response Process–Not all aspects of the Incident Response taxonomy are covered in this document. For example, the Detect Events Capability Area contains details of many detection capabilities that will provide input to the Incident Response process. Part of the evaluation process following event detection is to classify an event as an incident or attack. A security incident may pose a threat but the cause may be accidental. This is contrary to an attack where the threat is driven by intelligence value or gain, cost to implement, and intent. Therefore, the Organization will monitor for events with the understanding that incidents are a subset of events, and that attacks are a subset of incidents.

Monitor–See the Capability Interrelationships section for Monitoring Capabilities within the scope of the Gold Standard. Monitoring includes both technical and manual monitoring

where the latter includes people spotting anomalies within their work environment and notifying the appropriate chain of command for further investigation.
Detect–Detection is a trigger event within the monitoring process that results in a notification to the appropriate group for subsequent analysis. See the Capability Interrelationships section for Detect Capabilities within the scope of the Gold Standard.

Notify–Notification is both a process and an event, as well as both technical and manual. Effective notification requires awareness training for personnel and an established infrastructure to notify (e.g., help desk or CIRT). The Organization will simplify the notification process for the end-user community so that it includes one point of contact (i.e., help desk) and train help desk personnel in initial triage and escalation to CIRT.

Triage–Triage is a process of identifying event, incident, or attack characteristics to determine the actual or potential adverse effect and classification of the event as one of the following:

- Known event
- Unknown event
- Known incident
- Unknown incident
- Known attack
- Unknown attack

Known events, incidents, and attacks result in applying standard response procedures to expedite resolution. These standard response procedures may be executed by help desk staff or escalated to specialized groups (e.g., anti-virus). Identifying unknown events, incidents, and attacks quickly facilitates the investigation process to properly classify and treat the anomaly.

Escalate–Escalation is both a process and event resulting from the triage process. It is used when an incident or attack cannot be resolved using standard procedures. The help desk (or other primary contact point for end users) has formal procedures and well-defined points of contact for escalating event, incident, or attack details to subject matter experts (SMEs) or a response team.

Isolate–The first objective of the response team is to characterize and isolate the affected area, as appropriate. This may mean isolating a specific system by unplugging the network cable or isolating a network segment by reprogramming the routers to cut off all traffic flow. The appropriate isolation action is dependent on the severity of the anomaly

and evaluation of the overall impact to the mission. As noted in the Gold Standard definition, there may be times when no immediate action is taken.

Restore–The second objective is to restore mission functionality; this does not necessarily mean restoring the affected system or service. Every system or service produces a result that a consumer relies on. The IRT will be prepared ahead of time or quickly discover what result the affected system or service produces and how to produce that result from another source. This is the very nature of mission resiliency and continuing operations under adverse conditions. The contingency plan, continuity of operations plan (COOP), and disaster recovery plan will all provide insight into how to achieve this mission resiliency; however, technical redundancies are not the only solution. Effective mission resiliency requires both proactive and reactive creative lateral thinking to keep the mission operating.

Incident Response Outputs–Incident Response outputs include, but are not limited to, the following:

- Intelligence Analysis Reports
- National Security Information Systems Incident Program (NSISIP) Reports
- Effectiveness Reports, including effectiveness metrics
- Efficiency Reports, including efficiency metrics

The first level of Incident Response is where a majority of security incidents are handled by fully automated information exchange to rapidly and automatically execute actions that either ensure the continued defensive posture of the network or tip external organizations to employ their suite of capabilities to counter or exploit a threat. This approach relies heavily on threat awareness and intrusion detection and monitoring activities, linking the three together to automate finding, validating, and remedying the incident. The second level, partially automated, addresses incidents that require human intervention for risk assessment or authority to execute. The final level is manual, which addresses security incidents that cannot be addressed by the automated means. This level depends on the talent and expertise of Committee on National Security Systems (CNSS) analysts working in collaboration across the CNSS mission areas. The results of all response activities inform changes to the other two levels through the threat awareness and planning activities.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping–The Incident Response Capability relies on the Network Mapping Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Network Boundary and Interfaces–The Incident Response Capability relies on the Network Boundary and Interfaces Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Utilization and Performance Management–The Incident Response Capability relies on the Utilization and Performance Management Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Understand Mission Flows–The Incident Response Capability relies on the Understand Mission Flows Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Understand Data Flows–The Incident Response Capability relies on the Understand Data Flows Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Hardware Device Inventory–The Incident Response Capability relies on the Hardware Device Inventory Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Software Inventory–The Incident Response Capability relies on the Software Inventory Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.

- Understand the Physical Environment–The Incident Response Capability relies on the Understand the Physical Environment Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Configuration Management–The Incident Response Capability relies on the Configuration Management Capability for information used to know what software patches and configurations are available to assess whether patching or reconfiguring should be part of possible courses of action.
- Network Security Evaluations–The Incident Response Capability relies on the Network Security Evaluations Capability as a source of incident notifications to be addressed.
- Vulnerability Assessment–The Incident Response Capability relies on the Vulnerability Assessment Capability to provide prioritized vulnerability alerts.
- Threat Assessment–The Incident Response Capability relies on the Threat Assessment Capability for information used to make adjustments to its functions as the characteristics of threats directed against the Enterprise change over time.
- Network Enterprise Monitoring–The Incident Response Capability relies on the Network Enterprise Monitoring Capability for information used to make adjustments to its functions in response to potential problems detected and under review.
- Physical Enterprise Monitoring–The Incident Response Capability relies on the Physical Enterprise Monitoring Capability for information used to make adjustments to its functions in response to potential problems detected and under review.
- Personnel Enterprise Monitoring–The Incident Response Capability relies on the Personnel Enterprise Monitoring Capability for information used to make adjustments to its functions in response to potential problems detected and under review.
- Network Intrusion Detection–The Incident Response Capability relies on the Network Intrusion Detection Capability for information used to make adjustments to its functions in response to potential problems detected and under review.
- Host Intrusion Detection–The Incident Response Capability relies on the Host Intrusion Detection Capability for information used to make adjustments to its functions in response to potential problems detected and under review.
- Network Hunting–The Incident Response Capability relies on the Network Hunting Capability for information used to make adjustments to its functions in response to potential problems detected and under review.

- Physical Hunting–The Incident Response Capability relies on the Physical Hunting Capability for information used to make adjustments to its functions in response to potential problems detected and under review.
- Enterprise Audit Management–The Incident Response Capability relies on the Enterprise Audit Management Capability for information used to make adjustments to its functions in response to potential problems detected and under review.
- Network Intrusion Prevention–The Incident Response Capability relies on the Network Intrusion Prevention Capability for information used to make adjustments to its functions based on intrusion prevention response activities.
- Host Intrusion Prevention–The Incident Response Capability relies on the Host Intrusion Prevention Capability for information used to make adjustments to its functions based on intrusion prevention response activities.
- Contingency Planning–The Incident Response Capability relies on the Contingency Planning Capability for information used to make adjustments to its functions based on contingency response activities.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Incident Response Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Incident Response Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable Federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness–The Incident Response Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Incident Response Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Incident Response Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Physical and Environmental Protections–The Incident Response Capability relies on the Physical and Environmental Protections Capability for information used to assess the results of its response to specific incidents.
- Risk Mitigation–The Incident Response Capability relies on the Risk Mitigation Capability for information used to make adjustments to its functions as the Enterprise risk posture and appropriate countermeasures change over time.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
IR-1 *INCIDENT RESPONSE POLICY AND PROCEDURES*	Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. Enhancement/s: None Specified
IR-3 *INCIDENT RESPONSE TESTING AND EXERCISES*	Control: The organization tests and/or exercises the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results. Enhancement/s: (1) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response

	capability.
IR-4 *INCIDENT HANDLING*	Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. Enhancement/s: (1) The organization employs automated mechanisms to support the incident handling process. (2) The organization includes dynamic reconfiguration of the information system as part of the incident response capability. (5) The organization implements a configurable capability to automatically disable the information system if any of the following security violations are detected: [Assignment: organization-defined list of security violations].
IR-6 *INCIDENT REPORTING*	Control: The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time-period]; and b. Reports security incident information to designated authorities. Enhancement/s: (1) The organization employs automated mechanisms to assist in the reporting of security incidents. (2) The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.
IR-7 *INCIDENT RESPONSE ASSISTANCE*	Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents. Enhancement/s: (1) The organization employs automated mechanisms to

	increase the availability of incident response-related information and support. (2) The organization: (a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and (b) Identifies organizational incident response team members to the external providers.
IR-8 *INCIDENT RESPONSE PLAN*	Control: The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; -Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational

	elements]. Enhancement/s: None Specified.
SI-3 *MALICIOUS CODE PROTECTION*	Control: The organization: d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Enhancement/s: (6) The organization tests malicious code protection mechanisms [Assignment: organization-defined frequency] by introducing a known benign, non-spreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required.

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Incident Response Directives and Policies

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
ICD 503 IC Information Technology Systems Security Risk Management, Certification and Accreditation, Effective 15 September 2008, Unclassified	Summary: Incident Response is a part of the System Security Plan (template) required for risk management and certification and accreditation.
ICPG 503.1 Information and Information Systems Governance Roles and Responsibilities (DRAFT), October 2007, Unclassified	Summary: This Draft IC Policy Guidance includes a Chief Information Officer (CIO) responsibility to: Establish procedures for detecting, reporting, and responding to network security incidents.
Intelligence Community Policy for Reporting Security Incidents and Outages on Intelligence	Summary: This Intelligence Community (IC) policy establishes both policy and responsibilities for Incident Management including both response and analysis.

Community Information Systems, 26 April 2004, Classified	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
DNI Memorandum E/S 00765, Concept of Operations and Plan for Implementation of the Comprehensive National Cybersecurity Initiative to Connect Current Cyber Centers, Classified	Summary: This document is classified and addresses Incident Response.
Department of Defense (DoD)	
DoDD 3020.40, DoD Policy and Responsibilities for Critical infrastructure, Incorporating change 1, 1 July 2010, Unclassified	Summary: This directive sets policy that Defense critical infrastructure risk management actions shall support incident management.
DoDI 3020.45, Defense Critical Infrastructure Program (DCIP) Management, 21 April 2008, Unclassified	Summary: This instruction implements an established policy in support of Department of Defense Directive (DoDD) 3020.40, 40, DoD Policy and Responsibilities for Critical infrastructure, including supporting incident management. It creates policy that appropriate Defense Critical infrastructure Program (DCIP) information shall be provided to incident management officials responding to incidents and identifies responsibilities.
DoDI 8410.02 NetOps for the Global Information Grid (GIG), 19 December 2008, Unclassified	Summary: This instruction sets policy: 4. c. Global Information Grid (GIG) Enterprise Management (GEM), GIG Net Assurance (GNA), and GIG Content Management (GCM) functions shall be operationally and

	technically integrated to ensure simultaneous and effective monitoring, management, and security of the Enterprise. This instruction sets responsibility: 9. c. Coordinate intelligence and information sharing activities involving DoD SCI networks with the IC Incident Response Center (IRC) in accordance with the established procedures approved by the Secretary of Defense and the DNI or their designees pursuant to Reference…
DoDD 8500.01E Information Assurance (IA), 23 April 2007, Unclassified	Summary: This Directive sets policy for interoperability and integration of information assurance (IA)…to include incident detection and response.
DoDD O-8530.1 Computer Network Defense (CND), 8 January 2001, Classified	Summary: It is DoD policy that: 4.1. All DoD information systems and computer networks shall be monitored… isolate and react to intrusions, disruptions of services, or other incidents …
DoD 8580.02-R DoD Health Information Security Regulation, 12 July 2007, Unclassified	Summary: This regulation sets policy for the heads of DoD components to provide for an Incident Response and reporting capability.
CJCSI 6510.01E Information Assurance (IA) and Computer Network Defense (CND), current as of 12 August 2008, Unclassified	Summary: This instruction assigns responsibilities for Incident Response and Incident Response assessment reports. The Chief of the Joint Chiefs of Staff Manual (CJCSM) 6510.01A provides additional information on the DoD incident handling program.
CJCSM 6510.01A, Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program), 24 June 2009, Unclassified	Summary: This manual describes the DoD Incident Handling Program, the major processes that take place within the incident handling program, and the interactions with related U.S government CND activities. The manual provides high-level guidance for implementing the DoD Incident Handling Program.
Committee for National Security Systems (CNSS)	
CNSSI-1001, National Instruction on Classified Information Spillage,	Summary: This instruction establishes procedures: 5. When there is evidence of a possible spillage of classified national security information, hereinafter "classified

February 2008, Unclassified	information," an immediate notification shall be made to the information owner, the Information Assurance Manager (IAM), the Activity Security Manager, and the responsible IRC…
CNSSP-18 National Policy on Classified Information Spillage, June 2006, Unclassified	Summary: This policy established national policy: 5.a. Reported to the appropriate authorities. These authorities shall minimally include the information owner, the IAM/Information System Security Manager (ISSM), the Activity Security Manager, and the responsible IRC...
CNSS-048-07 National Information Assurance (IA) Approach to Incident Management (IM), May 2007, Unclassified	Summary: This Committee on National Security Systems (CNSS) issuance is mainly informational and is NOT binding on U.S. government departments and agencies. It describes an Incident Management program approach versus a response approach. It seeks to promote a more cohesive approach to capitalize on existing and new strategic partnerships throughout the government and private sectors.
CNSS-079-07 Frequently Asked Questions (FAQ) on Incidents and Spills, August 2007, Unclassified	Summary: This Frequently Asked Questions (FAQ) issuance on Incidents and Spills is mainly informational and is NOT binding on U.S. government departments and agencies. It provides basic information on National Security Systems, Data Spills, and Incident Management.
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Incident Response Standards

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
DRAFT IC Standard 2008-xx Federal Information	Summary: Purpose: To standardize how member agencies of the IC report to the Associate Director National

Security Management ACT (FISMA) Compliance Reporting, 2008	Intelligence ADNI and CIO and the Office of the DNI Inspector General (ODNI/OIG) to meet the FISMA reporting requirements… This Draft Standard addresses Incident Reporting– IC members do not report directly to the U.S. Computer Emergency Response Team (US-CERT); incidents are reported to the Joint Task Force-Global Network Operations (JTF-GNO) (for DoD IC) and the IC/IRC, which, in turn, report to the US-CERT.
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
NIST SP 800-61 Rev 1 Computer Security Incident Handling Guide, March 2008, Unclassified	Summary: This publication seeks to assist organizations by providing practical guidelines on responding to incidents. The Incident Response has four main phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity.
NIST SP 800-83 Guide to Malware Incident Prevention and Handling, November 2005, Unclassified	Summary: This special publication provides recommendations for improving an Organization's malware incident prevention measures and gives extensive recommendations for enhancing existing Incident Response Capability so that it is better prepared to handle malware incidents, particularly widespread ones. Organizations should have a robust Incident Response process capability that addresses malware incident handling. During the detection and analysis phase, they should strive to detect and validate malware incidents rapidly by monitoring alerts produced by technical controls (e.g., antivirus software, spyware detection and removal utilities, intrusion detection systems) to identify likely impending malware incidents and

	risks associated with malware incidents.
NIST SP 800-86 Guide to Integrating Forensic Techniques Into Incident Response, April 2006, Unclassified	Summary: This publication helps organizations in investigating computer security incidents. The process for performing digital forensics contains the following phases: Collection, Examination, Analysis, and Reporting. This guide provides general recommendations for performing the forensic process.
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Travel expenses–The Incident Response Team may need to travel somewhere when an incident occurs.

2. Research costs–This Capability needs to know how to tailor standardized functions to meet the specialized needs of the Enterprise systems.
3. Number of connections–The more network and Internet connections in an Enterprise, the greater the amount of work the Incident Response Team will have to perform.
4. Infrastructure–The Incident Response Team will have to be able to operate in various environments that feature different facilities, computers, networks, voice equipment, software, and specialized technology.
5. Solution used for implementation–The Enterprise can establish the Incident Response Capability internally or use external contracts. If established internally, the Enterprise must provide the necessary tools for response.
6. Time to implement, maintain, and execute–Response processes can take time, especially if approval is needed to begin work.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Incident Response Capability.

- Incident response is a conscious plan of action given the stimulus of an assessed occurrence having actual or potentially adverse effects on an asset. It involves notification, triage, escalation, and isolation of technical, personnel, physical, and environmental incidents for the Enterprise, and restoration (when appropriate).
- The Enterprise shall have a program, staff, and plan to address incident response.
- All personnel involved with incident response activities shall be dedicated to this practice.
- There shall be pre-established communications channels from incident response personnel and systems to the personnel and systems that make decisions using the output from incident response activities.
- The incident response shall be able to response to incidents on a 24/7/365 basis.
- The incident response shall be able to respond to the full spectrum of technical, personnel, and physical and environmental incidents or attacks.
- Incident response activities shall be automated whenever possible. Semi-automated or manual responses shall be used when full automation is not possible.

- All procedures, roles, and responsibilities of users and incident response personnel shall be documented.
- The scope of incident response service shall be documented.
- Appropriate planning and analysis shall take place prior to conducting any incident response activities.
- The services offered by the incident response process shall be clearly enumerated.
- The consumers of incident response outputs shall be clearly identified and enumerated.
- Incident response personnel shall maintain a strict chain of custody for any physical evidence that is confiscated or modified.
- Incident response activities shall use real-time information including details of the technical infrastructure and what missions are affected.
- Incident response reports shall use a standard format to facilitate interoperability.
- Records of incidents shall be stored in a centrally managed repository for the Enterprise.
- Notification of an event, incident, or attack shall be responded to in near real-time (as they occur), when possible.
- A triage process shall assess characteristics of the event, incident, or attack to determine its actual or potential adverse effect (either incident or attack) and whether it has occurred before (known) or not (new).
- Responses applied to known incidents or attacks shall be reused to expedite response time.
- The Enterprise shall establish formal procedures to describe the escalation of incidents or attacks to specialists for review and resolution.
- The incident response team shall characterize the affected portion of the system and perform remediation steps, as necessary, including the possibility of isolating nodes from the rest of the network.
- Incident response activities shall restore mission functionality to the affected systems.
- Records and details on events, incidents, and attacks, and the response actions taken, shall be securely stored and accessible through a centrally managed data repository.